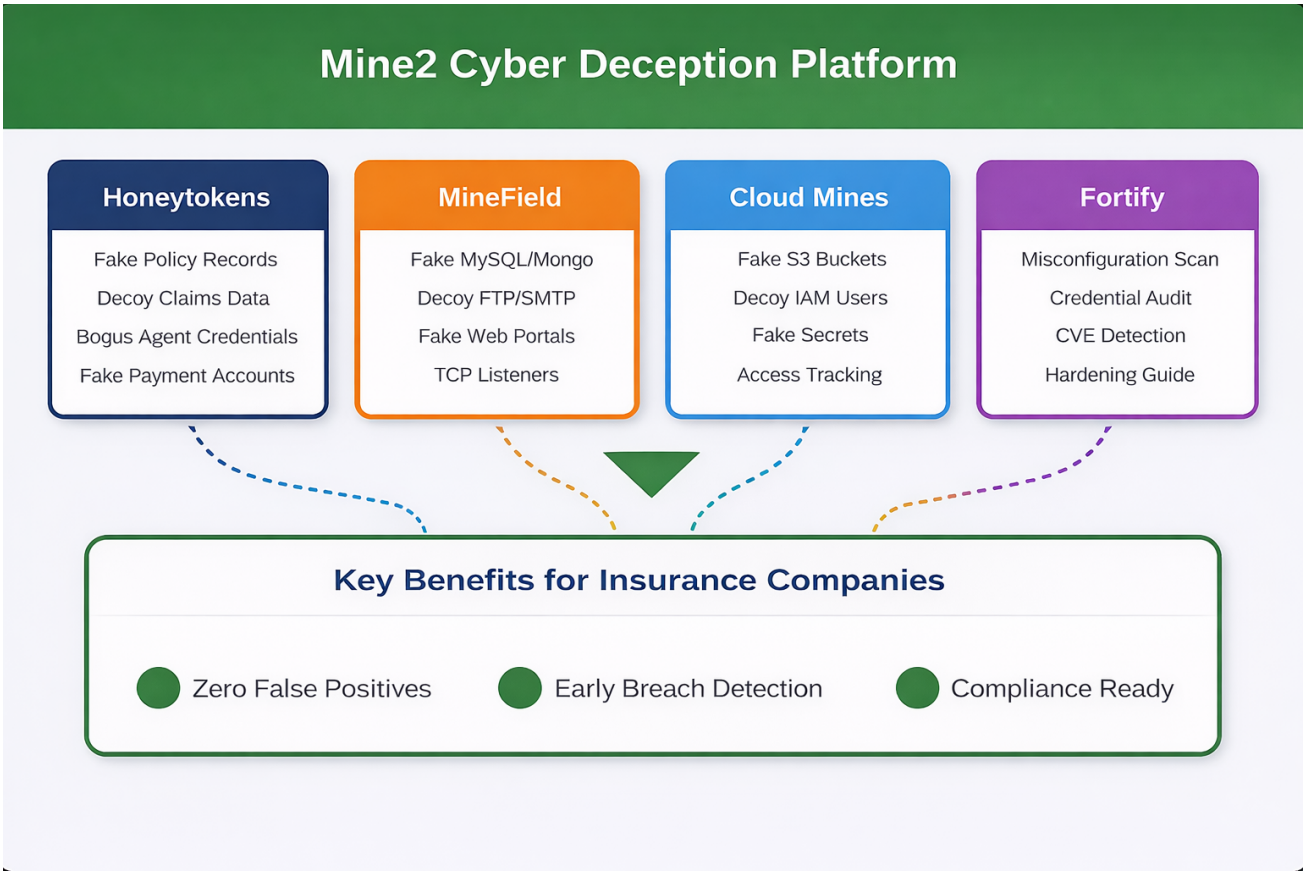
SECURING THE INSURANCE SECTOR

Cyber Deception Strategies for Universities and Colleges

A Mine2 Industry Whitepaper



www.mine2.io | info@mine2.io

Executive Summary

Insurance organizations process some of the most sensitive datasets in any industry, including identity records, medical histories, financial information, and payment details. Industry breach analyses consistently show that the financial and insurance sector experiences thousands of publicly disclosed data exposures annually, with identity and access misuse, cloud misconfigurations, and third-party compromises among the leading root causes. A single exposed storage bucket, leaked folder, or compromised vendor account can result in millions of records being accessible externally. Traditional perimeter and signature-based controls frequently fail to detect these exposures in real time. Mine2 introduces a deception-based detection layer that plants realistic decoys, honey credentials, and canary artifacts across endpoints, networks, and cloud environments to provide deterministic early-warning signals whenever an attacker touches assets they should never access.

The Challenge

According to global cybersecurity reports and regulatory advisories, the insurance sector consistently ranks among the most targeted industries for data breaches, fraud, and cyber intrusions due to the sensitivity and volume of data it processes. Several factors contribute to this elevated risk:

Highly Interconnected Ecosystems: Insurers operate complex environments spanning core policy systems, claims platforms, agent and broker portals, cloud services, and multiple third-party partners.
High-Value Sensitive Data: Large repositories of PII, financial information, medical records, payment details, and policy data make insurers attractive targets for attackers.
Operational & Regulatory Pressure: Continuous service availability, strict regulatory timelines, and compliance obligations limit the ability to take systems offline or aggressively modify legacy infrastructure.
Diverse Access Profiles: Employees, agents, brokers, TPAs, surveyors, and vendors access systems with varying levels of security awareness and privileges, increasing the risk of misuse or compromise.

Why Traditional Security Falls Short

Perimeter-focused: Assumes attackers are outside; fails against compromised credentials
Signature-based: Misses zero-day exploits and sophisticated APTs
Alert fatigue: Thousands of false positives overwhelm small teams
Late detection: Average dwell time exceeds 200 days

Mine2 Cyber Deception Platform

Honeytokens

Digital tripwires that alert when accessed: AWS/DB credentials, SSH/RDP keys, VPN configs, decoy documents (patient_details.xlsx), and AD user accounts.

MineField

Decoy network services: fake MySQL/MongoDB, FTP/SMTP servers, web portals, and IoT/CCTV interfaces. Any connection triggers immediate alerts.

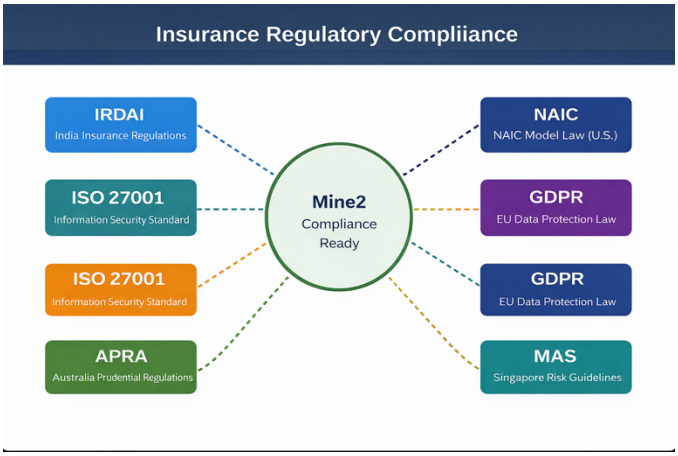
Cloud Mines

AWS deception: automated discovery, intelligent suggestions, and deployment of fake S3 buckets, IAM users, and secrets with access tracking.

Fortify

Proactive hardening: misconfiguration detection, credential audits, CVE scanning, and prioritized remediation guidance.

Regulatory Compliance



Key Use Cases

Ransomware & Lateral Movement Detection:
Detect attackers during lateral movement using decoy servers, credentials, and shares, enabling early containment before encryption or operational disruption.
Claims Fraud & Insider Threat Detection:
Honey policy records and fake payout accounts expose unauthorized access or manipulation, delivering high-confidence alerts for insider misuse and fraud prevention.
Agent/Broker Portal & Account Compromise Protection:
Honey accounts and hidden authentication endpoints reveal credential stuffing, phishing, and bot-driven login abuse before large-scale account takeover occurs.
Cloud & SaaS Data Exposure Prevention:
Honey files and canary tokens detect access to misconfigured S3 buckets, exposed folders, repositories, or directory paths with attacker attribution.
Supply Chain & Third-Party Risk Monitoring:
Deception assets in vendor-accessible environments detect compromised third-party credentials and supply-chain attacks at the earliest stage.
Social Engineering & Phishing Defense:
Seeded honey credentials identify successful phishing and credential reuse, triggering rapid response actions such as password resets and MFA enforcement.
Compliance & Audit Support:
Deterministic alerts and forensic telemetry support ISO 27001, SOC 2, GDPR, and insurance regulatory audit and breach reporting requirements.

Key Benefits

Near-Zero False Positives: Any honeytoken access = confirmed threat
Early Detection: Catch attackers in reconnaissance, not after damage

Low Overhead: No signatures, minimal tuning, no production impact, no resource bandwidth, no software dependencies
Non-Bypassable: Unlike EDR, Mines cannot be bypassed or identified in an environment
Insider Threat Detection: Same protection against external attackers and malicious insiders

Real-World Scenarios

1# An insurance agent falls victim to a **phishing** email, and their credentials are later used by an attacker to test access across multiple accounts. When the attacker attempts to log in using a Mine2 honey agent account and probes a hidden authentication endpoint, Mine2 detects credential abuse immediately. Security teams block the IP, reset affected credentials, and prevent large-scale agent account takeover.
2# A misconfigured cloud **bucket** containing policy documents and medical records is unintentionally **exposed**. Before attackers can access real data, a threat actor downloads a Mine2 honey document embedded with a canary token. The access triggers an alert with source IP and timestamp, enabling rapid remediation of the misconfiguration and preventing a reportable data breach.

3# A **disgruntled claims adjuster** tries to identify high-value claims and payout accounts for manipulation. While browsing internal databases, they access a fake SQL backup database and load it in hope to access sensitive records. Mine2 flags the activity instantly, providing clear evidence of unauthorized intent and enabling compliance and legal teams to intervene before financial loss occurs.

Getting Started

1. **Assessment:** Map critical assets and attack paths
2. **Planning:** Strategic placement of deception resources
3. **Deployment:** Days, not months—zero production impact
4. **Integration:** SIEM integration and team training
5. **Optimization:** Continuous coverage as environment evolves

Business Value

Reduced Breach Costs: Early detection prevents large-scale data exposure, significantly lowering breach remediation, legal fees, customer notification, and regulatory penalty costs.

Ransomware Impact Reduction: Detecting attackers before encryption avoids multimillion-rupee downtime losses across claims processing, underwriting, and customer service operations.

Lower Fraud Losses: Immediate detection of insider misuse and claims manipulation reduces direct financial leakage from fraudulent payouts and data monetization.

SOC Cost Optimization: Near-zero false positives reduce analyst time spent on triaging noisy alerts, allowing smaller teams to operate more efficiently without expanding headcount.

Minimal Deployment Overhead: Lightweight deception assets require no agents, no production traffic inspection, and no performance impact—eliminating infrastructure scaling and licensing costs.

Reduced Dependency on Heavy Tooling: Mine2 complements or offsets expensive SIEM, UEBA, and DLP tuning efforts by providing deterministic alerts instead of probabilistic detections.

Lower Compliance & Audit Spend: Built-in evidence, timestamps, and attacker attribution reduce audit preparation time, consultant costs, and compliance remediation cycles.

Third-Party Risk Cost Control: Early detection of vendor or TPA compromise prevents cascading incidents that typically lead to contract penalties, legal disputes, and reputational damage.

Legacy System Protection Without Replacement: Adds a security layer to aging underwriting and policy platforms without costly re-engineering or accelerated modernization projects.

Faster Incident Response: Reduced mean time to detect (MTTD) and respond (MTTR) directly lowers containment, forensic, and recovery expenses.

Improved Cyber-Insurance Posture: Strong detection and monitoring controls can support lower premiums and improved coverage terms from cyber insurers.

Business Continuity Assurance: Preventing service outages avoids revenue loss, SLA penalties, and customer churn during claims surges or renewal cycles.

Conclusion

Insurance organizations face increasingly sophisticated cyber threats while operating complex ecosystems of legacy systems, cloud platforms, agents, brokers, and third-party partners. Traditional, reactive security controls often leave blind spots that attackers exploit. Mine2's cyber deception acts as a force multiplier for insurance security teams—detecting breaches early with near-zero false positives while strengthening compliance with global insurance and data-protection regulations.

The question is not whether insurers will be targeted, but whether threats will be detected before policyholder data, claims operations, or business continuity are impacted. Mine2 ensures they are.

Contact Mine2 Today

www.mine2.io | info@mine2.io